(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－149023

(43)公開日　平成９年(1997)６月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ	9/16			Ｈ０４Ｌ	9/00	６４３
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｚ
		６６０	7259－5Ｊ			６６０Ｅ

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）

(21)出願番号　特願平7－305435

(22)出願日　平成７年(1995)11月24日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　馬場　信行
大阪府門真市大字門真1006番地　松下電器産業株式会社内

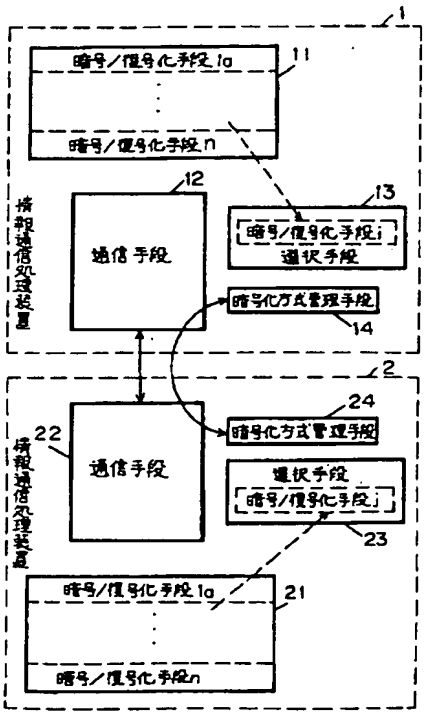
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　情報通信処理装置および情報通信処理方法

(57)【要約】

【課題】　解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理装置および情報通信処理方法を提供することを目的とする。

【解決手段】　複数の暗号／復号化手段をテーブル化した暗号化方式テーブル１１、２１と、暗号化方式テーブル１１、２１から所定の規則によって１つの暗号／復号化手段を選択する選択手段１３、２３と、選択された暗号／復号化手段の暗号化方式テーブル１１、２１のオフセット値を相手側へ通知する暗号化方式管理手段１４、２４とを有することにより、機密が漏洩する可能性が極めて小さい情報通信処理装置および情報通信処理方法が得られる。



1

【特許請求の範囲】

【請求項１】複数の暗号／復号化手段をテーブル化した暗号化方式テーブルと、前記暗号化方式テーブルから所定の規則によって１つの暗号／復号化手段を選択する選択手段と、前記選択された暗号／復号化手段の前記暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理手段とを有する情報通信処理装置。

【請求項２】前記暗号化方式管理手段は、自己側と相手側とで異なる前記オフセット値を保持する請求項１記載の情報通信処理装置。

【請求項３】前記暗号化方式管理手段は、定められた時間間隔で前記オフセット値を変更して相手側へ通知する請求項１記載の情報通信処理装置。

【請求項４】前記暗号化方式管理手段は、定められた時間間隔で、前記暗号化方式テーブルを変更し、前記変更された暗号化方式テーブルのオフセット値を選択し、前記変更された暗号化方式テーブルおよび前記選択されたオフセット値を相手側へ通知する請求項１記載の情報通信処理装置。

【請求項５】複数の暗号化方式テーブルから所定の規則によって１つの暗号／復号化手段を選択する選択ステップと、前記選択された暗号／復号化手段の前記暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理ステップとを有する情報通信処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クレジット番号や機密文書等の文字データや画像／音声データを交換する情報通信処理装置および情報通信処理方法に関する。

【０００２】

【従来の技術】近年、社会機構が複雑になるに伴い、機密文書等の漏洩防止の要請が高まりつつある。ところで、従来の情報通信処理装置では、扱うデータを暗号化しなかったり、単数もしくは複数の固定の暗号化方式で暗号化していた。また、同一のネットワーク内では同じ暗号化方式を利用する場合が多い。

【０００３】

【発明が解決しようとする課題】しかしながら、上記の従来の情報通信処理装置では、機密漏洩防止を防止するのに十分な暗号化方式が使用されておらず、一部又はすべてのデジタルデータや音声データ、画像データが漏洩する可能性が大きいという問題点を有していた。

【０００４】この情報通信処理装置においては、解読困難で機密漏洩の可能性が少ないことが要求されている。

【０００５】本発明は、解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理装置および解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】この目的を達成するため

2

に本発明は、複数の暗号／復号化手段をテーブル化した暗号化方式テーブルと、暗号化方式テーブルから所定の規則によって１つの暗号／復号化手段を選択する選択手段と、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理手段とを有するように構成したものである。

【０００７】これにより、解読が困難なことにより機密が漏洩する可能性が極めて小さい情報通信処理装置が得られる。

【０００８】

【発明の実施の形態】本発明の請求項１に記載の発明は、複数の暗号／復号化手段をテーブル化した暗号化方式テーブルと、暗号化方式テーブルから所定の規則によって１つの暗号／復号化手段を選択する選択手段と、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理手段とを有することとしたものであり、送信側で暗号化方式が任意に変更されるという作用を有する。

【０００９】請求項２に記載の発明は、請求項１に記載の発明において、暗号化方式管理手段が自己側と相手側とで異なるオフセット値を保持することとしたものであり、接続された情報通信処理装置は互いに独立した暗号化方法で送信するという作用を有する。

【００１０】請求項３に記載の発明は、請求項１に記載の発明において、暗号化方式管理手段が定められた時間間隔でオフセット値を変更して相手側へ通知することとしたものであり、定期的に暗号化方式が変更されるという作用を有する。

【００１１】請求項４に記載の発明は、請求項１に記載の発明において、暗号化方式管理手段が、定められた時間間隔で、暗号化方式テーブルを変更し、変更された暗号化方式テーブルのオフセット値を選択し、変更された暗号化方式テーブルおよび選択されたオフセット値を相手側へ通知することとしたものであり、定められた時間間隔で暗号化方式テーブルのオフセット値のみならず暗号化方式テーブルをも変更されるという作用を有する。

【００１２】請求項５に記載の発明は、複数の暗号化方式テーブルから所定の規則によって１つの暗号／復号化手段を選択する選択ステップと、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を相手側へ通知する暗号化方式管理ステップとを有することとしたものであり、送信側で暗号化方式を任意に変更されるという作用を有する。

【００１３】以下、本発明の実施の形態について、図１から図９を用いて説明する。

（実施の形態１）図１は本発明の一実施の形態に係る情報通信処理装置を示すブロック図である。

【００１４】図１において、１、２は機密文書等の文字データや画像／音声データを交換する情報通信処理装置、１１、２１は情報通信処理装置１、２の暗号／復号

化手段をテーブル化し、同一の内容を持つ暗号化方式テーブル、１２、２２は暗号化されたデータを送受信する通信手段、１３、２３は暗号／復号化手段を選択して格納する選択手段、１４、２４は選択された暗号／復号化手段を一方から他方へ、または相互に通知する暗号化方式管理手段である。暗号／復号化手段とは暗号化および復号化を行う手段であり、暗号化方式テーブル１１、２１のオフセット値で特定され、情報通信処置装置１、２のそれぞれを構成するノードのリンク数だけ存在する。オフセット値とは図１に示す１ａ、ｉ、ｎといった番号値である。

【００１５】以上のように構成された情報通信処理装置について、以下その動作を図２を用いて説明する。図２（ａ）は本実施の形態の動作を説明するための送信側のフローチャート、図２（ｂ）は本実施の形態の動作を説明するための受信側のフローチャートである。まず図２（ａ）に示す送信側の情報通信処理装置の動作について説明する。ここでは情報通信処理装置１を送信側、情報通信処理装置２を受信側とする。送信側の選択手段１３は、利用者の指定または利用者が定めた何らかの規則により、暗号化方式テーブル１１から１つの暗号／復号化手段を選択する（Ｓ１、選択ステップ）。利用者が定めた何らかの規則とは、例えば１セッション間毎に暗号化方法を切り替えるといったような規則である。次に、暗号化方式管理手段１４は、選択手段１３で選択した暗号／復号化手段の暗号化方式テーブル１１のオフセット値を記憶し、通信手段１２を使って、接続する相手側（受信側）の情報通信処理装置２に通知する（Ｓ２、暗号化方式管理ステップ）。次に、暗号化方式管理手段１４は、以後のデータ送受信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う（Ｓ３）。

【００１６】次に、図２（ｂ）に示す受信側の情報通信処理装置２の動作について説明する。暗号化方式管理手段２４は、通信手段２２によって受信した暗号化方式テーブル１１のオフセット値を記憶し、選択手段２３は暗号化方式テーブル２１から対応する暗号／復号化手段を選択する（Ｓ１１）。次に、暗号化方式管理手段２４は、以後のデータ送受信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う（Ｓ１２）。

【００１７】このように本実施の形態１では、送信側で指定した暗号化方式に従って、送信側および受信側の情報通信処理装置１、２は情報の通信処理（暗号化および復号化の処理）を行う。すなわち、情報通信処理装置１、２は共に同じ暗号化方式で通信処理を行う。

【００１８】以上のように本実施の形態１によれば、送信側で暗号化方式を任意に変更することができるので、情報の通信処理における機密保護レベルを向上させることが可能となる。

【００１９】（実施の形態２）第２の実施の形態に係る情報通信処理装置の構成は図１と同じであるが、動作が異なる。

【００２０】以上のように構成された第２の実施の形態に係る情報通信処理装置について、その動作を図３、図４を用いて説明する。図３は第２の実施の形態の動作を概略示す概略動作説明図であり、図４は第２の実施の形態の動作を説明するためのフローチャートである。

【００２１】図３は情報通信処理装置１、２間でデータ通信を行った場合の時間的推移を示す。時間ｔ１～ｔ２の送受信において、それぞれ異なる暗号化方式（１）、（２）によってデータ通信を行っている。

【００２２】図４により、第２の実施の形態の動作を詳細に説明する。まず選択手段１３、２３は、利用者または利用者が定めた何らかの規則により、暗号化方式テーブル１１、２１から１つの暗号／復号化手段を選択する（Ｓ２１）。次に、暗号化方式管理手段１４、２４は、選択手段１３、２３で選択した暗号／復号化手段の暗号化方式テーブル１１、２１のオフセット値を記憶し、通信手段１２、２２を使って、接続する相手側の情報通信処理装置１、２に通知する（Ｓ２２）。暗号化方式管理手段１４、２４は、相手側情報通信処理装置１、２への以後のデータ送信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う（Ｓ２３）。次に、暗号化方式管理手段１４、２４は、通信手段１２、２２によって相手側装置１、２より受信した暗号化方式テーブル２１、１１のオフセット値を記憶し、選択手段１３、２３は暗号化方式テーブル１１、２１から対応する暗号／復号化手段を選択する（Ｓ２４）。暗号化方式管理手段１４、２４は、相手側情報通信処理装置１、２からの以後のデータ受信に関し、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う（Ｓ２５）。

【００２３】以上のように第２の実施の形態によれば、接続された情報通信処理装置１、２は互いに独立した暗号化方法で送信することができるので、互いに送信する暗号化方法を異なるものとすることができ、暗号解読を一層困難なものとすることができ、機密保護レベルを一層向上させることが可能となる。

【００２４】（実施の形態３）第３の実施の形態に係る情報通信処理装置の構成は図１と同じであるが、動作が異なる。

【００２５】以下、その動作について図５、図６、図７を用いて説明する。図５は第３の実施の形態の動作を概略示す概略動作説明図であり、図６、図７は第３の実施の形態の動作を送信側、受信側について説明するためのフローチャートである。

【００２６】図５は情報通信処理装置１、２間でデータ通信を行った場合の時間的推移を示す。時間ｔ１～ｔ２、ｔ２～ｔ３、ｔ３～ｔ４において、それぞれ異なる

暗号化方式（１）、（２）、（３）によってデータ通信を行っている。

【００２７】図６により、第３の実施の形態の動作を送信側について詳細に説明する。図６は接続後の送信側情報通信処理装置における通信処理動作を示し、また、ここでは情報通信処理装置１を送信側、情報通信処理装置２を受信側とする。まず判別手段としての暗号化方式管理手段１４は、あらかじめ利用者に設定された暗号／符号化手段を切り替える、つまり暗号化方式を切り替えるタイミングか否かを判定する（Ｓ３１）。切り替えるタイミングでない場合には待機状態となる。切り替えるタイミングの場合には、暗号化方式管理手段１４は、あらかじめ利用者により指定された暗号／復号化手段の暗号化方式テーブル１１のオフセット値を記憶し、通信手段１２を使って接続する相手側（受信側）情報通信処理装置２に通知する（Ｓ３２）。暗号化方式管理手段１４は、相手側情報通信処理装置２との以後のデータ送受信に関し、指定した暗号／復号化手段を使ってデータの暗号化および復号化を行う（Ｓ３３）。

【００２８】図７により、第３の実施の形態の動作を受信側について詳細に説明する。図７は接続後の受信側情報通信処理装置２における通信処理動作を示す。まず暗号化方式管理手段２４は通信手段２２によって受信した暗号化方式テーブル１１のオフセット値を記憶し、選択手段２３は暗号化方式テーブル２１から対応する暗号／復号化手段を選択する（Ｓ４１）。暗号化方式管理手段２４は、相手側情報通信処理装置１との以後のデータ送受信に関し、暗号化方式テーブル２１上の選択された暗号／復号化手段（すなわち暗号化方式テーブル１１上の指定された暗号／復号化手段）を使ってデータの暗号化および復号化を行う（Ｓ４２）。

【００２９】以上のように第３の実施の形態によれば、あらかじめ利用者に設定された暗号／符号化手段切替えのタイミングで暗号／復号化手段を切り替える、すなわち定められた時間間隔でオフセット値を変更することにより、暗号解読を益々困難なものとすることができるので、機密保護レベルを益々向上させることが可能となる。

【００３０】（実施の形態４）第４の実施の形態に係る情報通信処理装置の構成は図１と同じであるが、動作が異なる。

【００３１】以下、その動作について図８、図９を用いて説明する。図８、図９は第４の実施の形態の動作を送信側、受信側について説明するためのフローチャートである。

【００３２】図８により、第４の実施の形態の動作を送信側について説明する。図８は接続後の送信側情報通信処理装置１における通信処理動作を示し、また、ここでは情報通信処理装置１を送信側、情報通信処理装置２を受信側とする。まず判別手段としての暗号化方式管理手段１４は、あらかじめ利用者に設定された暗号／符号化手段を切り替える、つまり暗号化方式を切り替えるタイミングか否かを判定する（Ｓ５１）。切り替えるタイミングでない場合には待機状態となる。切り替えるタイミングの場合には、暗号化方式管理手段１４は、あらかじめ利用者により指定された暗号化方式テーブル（変更された新たな暗号化方式テーブル）を記憶し、さらに、選択された暗号／復号化手段の上記新たな暗号化方式テーブルのオフセット値を記憶し、指定された新たな暗号化方式テーブルおよび新たな暗号化方式テーブル上の選択されたオフセット値を通信手段１２を使って接続する相手側（受信側）情報通信処理装置２に通知する（Ｓ５２）。暗号化方式管理手段１４は、相手側情報通信処理装置２との以後のデータ送受信に関し、指定された暗号化方式テーブル上の選択された暗号／復号化手段を使ってデータの暗号化および復号化を行う（Ｓ５３）。

【００３３】図９により、第４の実施の形態の動作を受信側について説明する。図９は接続後の受信側情報通信処理装置２における通信処理動作を示す。まず暗号化方式管理手段２４は通信手段２２によって受信した上記新たな暗号化方式テーブルを記憶する（Ｓ６１）。次に、暗号化方式管理手段２４は通信手段２２によって受信した上記新たな暗号化方式テーブル上の選択されたオフセット値を記憶し、選択手段２３は暗号化方式テーブル２１から対応する暗号／復号化手段を選択する（Ｓ６２）。暗号化方式管理手段２４は、相手側情報通信処理装置１との以後のデータ送受信に関し、指定された新たな暗号化方式テーブル上の選択された暗号／復号化手段を使ってデータの暗号化および復号化を行う（Ｓ６３）。

【００３４】以上のように第４の実施の形態によれば、あらかじめ利用者に設定された暗号／符号化手段切替えのタイミングで暗号／復号化手段のみならず暗号化方式テーブルをも切り替える、すなわち定められた時間間隔で暗号化方式テーブルのオフセット値のみならず暗号化方式テーブルをも変更することにより、暗号解読を不可能なものとして万全の機密保護を図ることが可能となる。

【００３５】

【発明の効果】以上のように本発明の情報通信処理装置によれば、送信側で暗号化方式を任意に変更することができるので、情報の通信処理における機密保護レベルを向上させることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。また、接続された情報通信処理装置は互いに独立した暗号化方法で送信することができるので、互いに送信する暗号化方法を異なるものとすることができ、暗号解読を一層困難なものとすることができ、機密保護レベルを一層向上させることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。さらに、定期的に暗号化

方式を変更することができるので、暗号解読を益々困難なものとすることができ、機密保護レベルを益々向上させることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。さらに、定められた時間間隔で暗号化方式テーブルのオフセット値のみならず暗号化方式テーブルをも変更することができ、暗号解読を不可能なものとして万全の機密保護を図ることが可能な情報通信処理装置を実現することができるという有利な効果が得られる。

【００３６】本発明の情報通信処理方法によれば、送信側で暗号化方式を任意に変更することができるので、情報の通信処理における機密保護レベルを向上させることが可能な情報通信処理方法を実現することができるという有利な効果が得られる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る情報通信処理装置を示すブロック図

【図２】（ａ）本実施の形態の動作を説明するための送信側のフローチャート

（ｂ）本実施の形態の動作を説明するための受信側のフローチャート

【図３】第２の実施の形態の動作を概略示す概略動作説明図

【図４】第２の実施の形態の動作を説明するためのフローチャート

【図５】第３の実施の形態の動作を概略示す概略動作説明図

【図６】第３の実施の形態の動作を送信側について説明するためのフローチャート

【図７】第３の実施の形態の動作を受信側について説明するためのフローチャート

【図８】第４の実施の形態の動作を送信側について説明するためのフローチャート

【図９】第４の実施の形態の動作を受信側について説明するためのフローチャート

【符号の説明】

１、２　情報通信処理装置

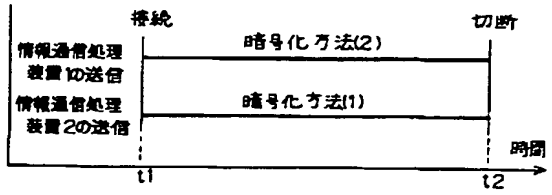
１１、２１　暗号化方式テーブル

１２、２２　通信手段

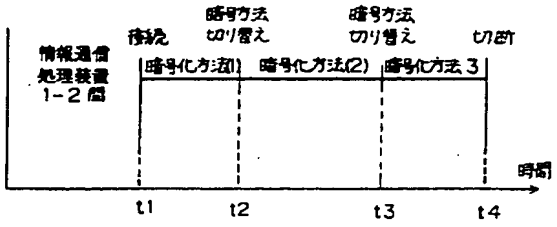
１３、２３　選択手段

１４、２４　暗号化方式管理手段

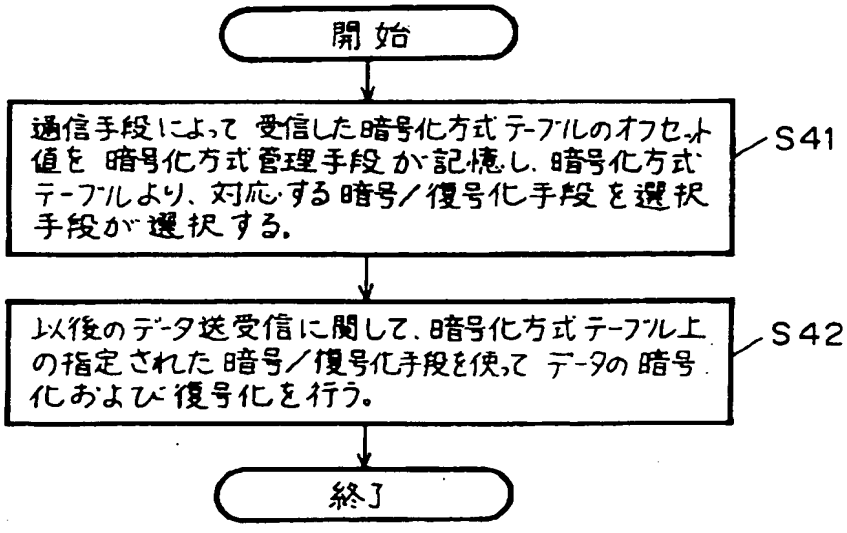
【図３】



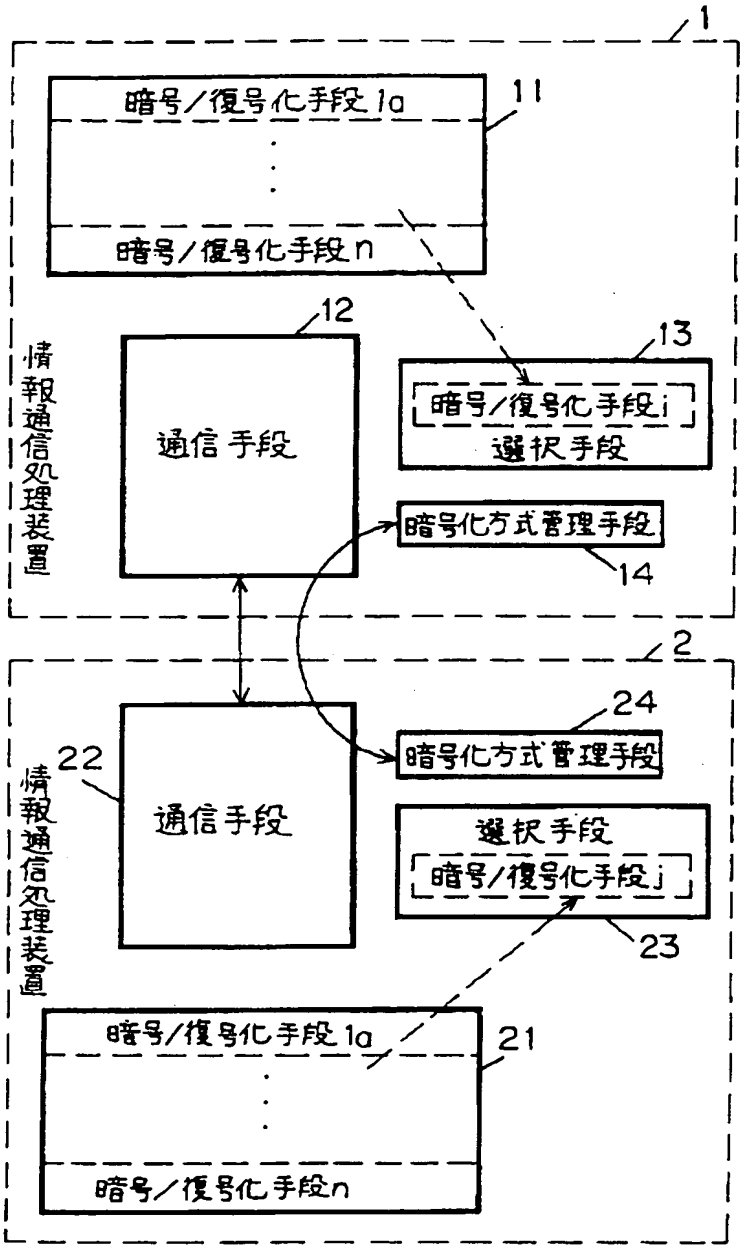
【図５】



【図７】

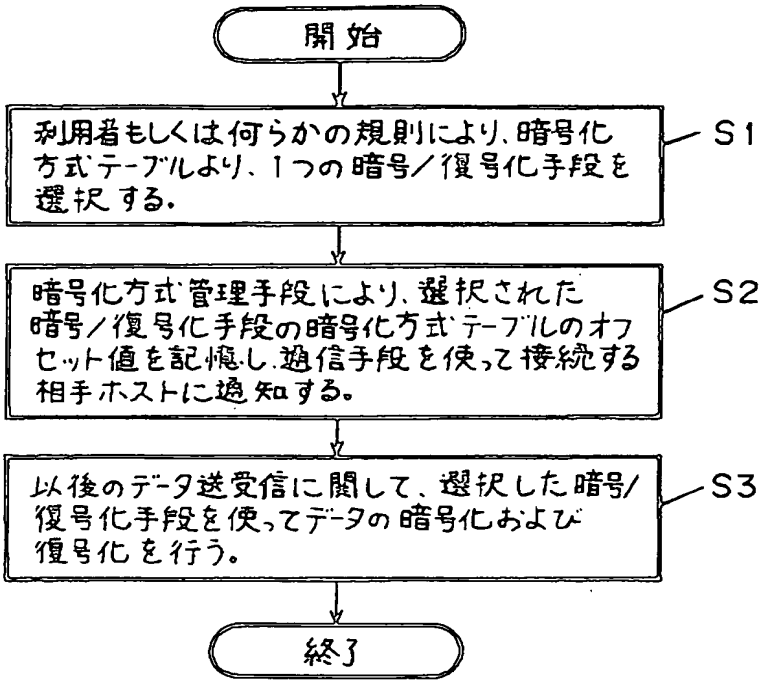


【図1】

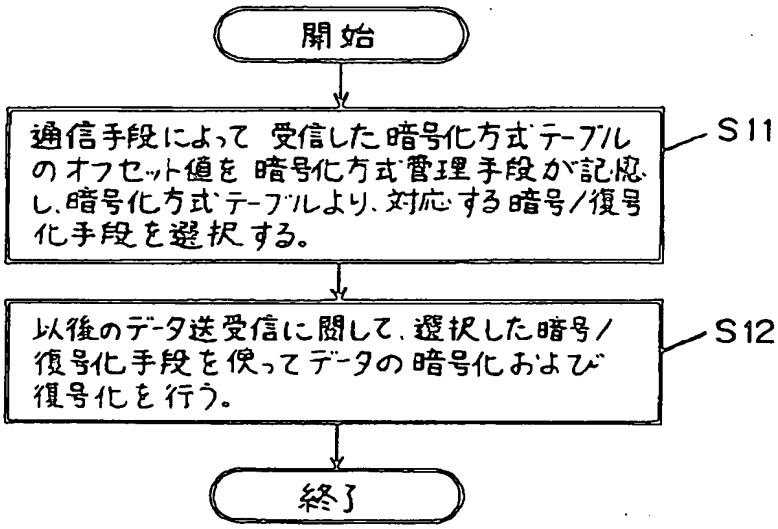

1
暗号/復号化手段1a
11
暗号/復号化手段n
12
13
情報通信処理装置
通信手段
暗号/復号化手段i
選択手段
暗号化方式管理手段
14
2
24
22
暗号化方式管理手段
情報通信処理装置
通信手段
選択手段
暗号/復号化手段j
23
暗号/復号化手段1a
21
暗号/復号化手段n

【図２】

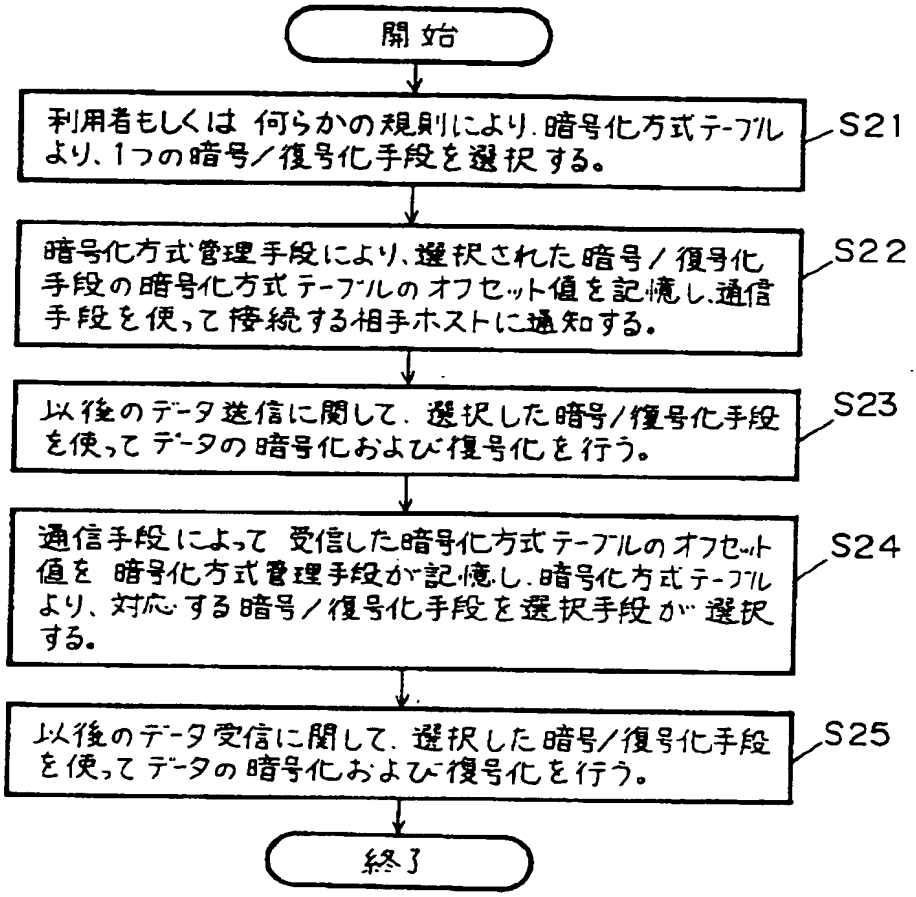
(a)


開始
利用者もしくは何らかの規則により、暗号化方式テーブルより、１つの暗号／復号化手段を選択する。
S1
暗号化方式管理手段により、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を記憶し、通信手段を使って接続する相手ホストに通知する。
S2
以後のデータ送受信に関して、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う。
S3
終了

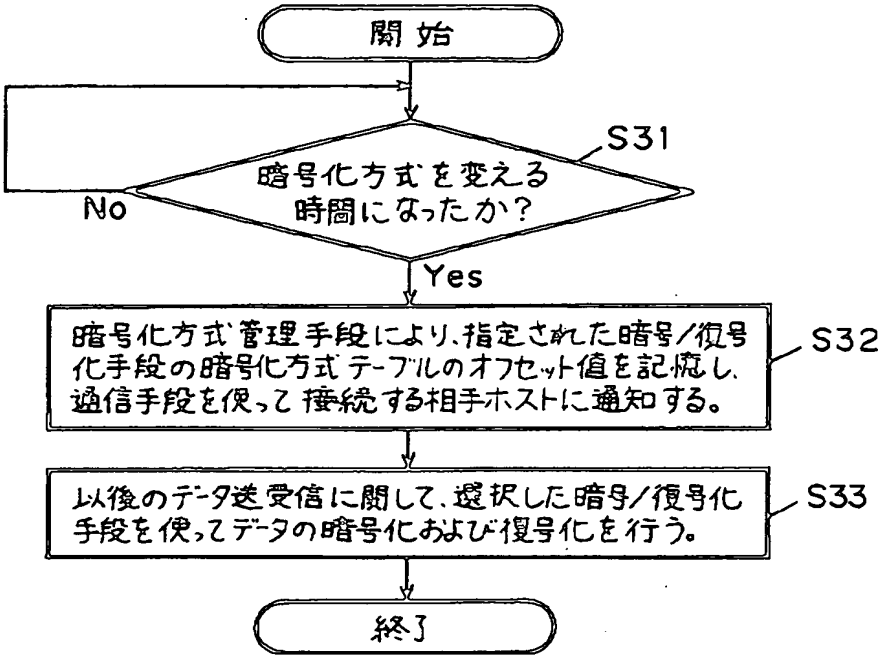
(b)


開始
通信手段によって受信した暗号化方式テーブルのオフセット値を暗号化方式管理手段が記憶し、暗号化方式テーブルより、対応する暗号／復号化手段を選択する。
S11
以後のデータ送受信に関して、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う。
S12
終了

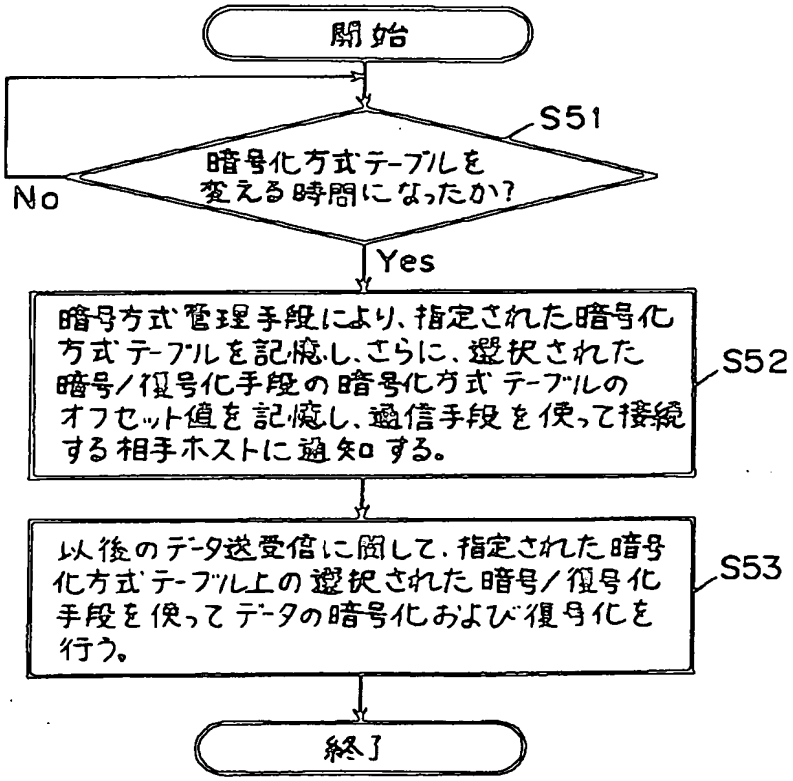
【図4】


開始
利用者もしくは 何らかの規則により、暗号化方式テーブルより、1つの暗号／復号化手段を選択する。
S21
暗号化方式管理手段により、選択された暗号／復号化手段の暗号化方式テーブルのオフセット値を記憶し、通信手段を使って接続する相手ホストに通知する。
S22
以後のデータ送信に関して、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う。
S23
通信手段によって 受信した暗号化方式テーブルのオフセット値を 暗号化方式管理手段が記憶し、暗号化方式テーブルより、対応する暗号／復号化手段を選択手段が選択する。
S24
以後のデータ受信に関して、選択した暗号／復号化手段を使ってデータの暗号化および復号化を行う。
S25
終了

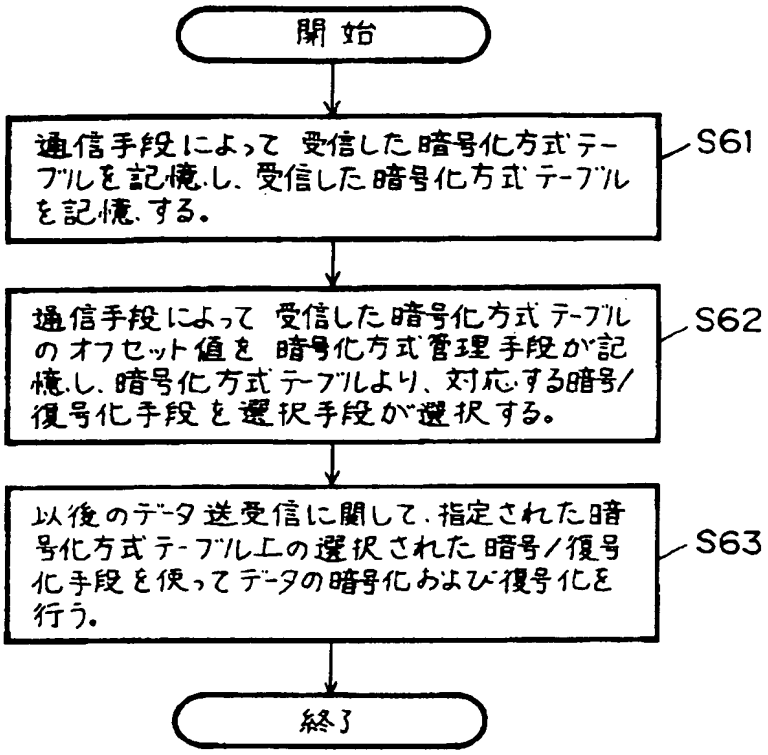
【図6】


開始
S31
暗号化方式を変える時間になったか?
No
Yes
暗号化方式管理手段により、指定された暗号/復号化手段の暗号化方式テーブルのオフセット値を記憶し、通信手段を使って接続する相手ホストに通知する。
S32
以後のデータ送受信に関して、選択した暗号/復号化手段を使ってデータの暗号化および復号化を行う。
S33
終了

【図8】


開始
S51
暗号化方式テーブルを変える時間になったか?
No
Yes
暗号方式管理手段により、指定された暗号化方式テーブルを記憶し、さらに、選択された暗号/復号化手段の暗号化方式テーブルのオフセット値を記憶し、通信手段を使って接続する相手ホストに通知する。
S52
以後のデータ送受信に関して、指定された暗号化方式テーブル上の選択された暗号/復号化手段を使ってデータの暗号化および復号化を行う。
S53
終了

【図９】


開始
通信手段によって 受信した暗号化方式テーブルを記憶し、受信した暗号化方式テーブルを記憶する。
S61
通信手段によって 受信した暗号化方式テーブルのオフセット値を 暗号化方式管理手段が記憶し、暗号化方式テーブルより、対応する暗号/復号化手段を選択手段が選択する。
S62
以後のデータ送受信に関して、指定された暗号化方式テーブル上の選択された暗号/復号化手段を使ってデータの暗号化および復号化を行う。
S63
終了